

AMENDMENTS TO THE SPECIFICATION

Please replace paragraph [0006] with the following paragraph:

[0006] The invention relates to computer-based methods and systems for time-based authentication that offer increased resistance to attack by generating different dynamic authentication codes within a single time interval. Each authentication code is generated using a generation value, which is different for generation attempts within a time interval. In one embodiment, a combination function is employed that takes as input a secret, a dynamic value, a PIN value, and a generation value. (The combination function may also take as input a verifier identifier as well as other information.) Each authentication attempt during the same time interval uses a different generation value and, in some embodiments, the receipt of the PIN triggers a change in the generation value. Use of this generation value in the combination function makes it more difficult for an attacker to attack the system by generating or observing the generation of multiple authentication codes within a time[[r]] interval, because information that previously was available to the attacker in the prior art systems is now hidden.

Please replace paragraph [0033] with the following paragraph:

[0033] The stored secret (K) is a unit of information such as a numerical value that is uniquely associated with, and typically manufactured into, the device 120. In one particular embodiment, the secret (K) is 128 bits in length. In a typical hardware implementation of the device 120, the secret (K) is stored inside the device 120 such that it is very difficult to extract the secret (K) from the device. In a typical software implementation of the device 120, the secret (K) is preferably stored in a secure data store accessible to the device 120. In addition to being accessible to the device 120, the secret (K) is also stored in a secure data store accessible to the verification computer 150. In other embodiments the secret (K) may be derived from a master secret (K_{MASTER}), as described in ~~co-pending application serial no. 09/304,775~~ U.S. Patent No. 6,985,583, the contents of which are incorporated herein by reference. The secret is preferably a value that is chosen from a large number of possible values such that it would be difficult for an opponent who had access to the output of the combination function 130 to guess the secret by trying each possible secret value to see if it resulted in the observed authentication code.

Please replace paragraph [0046] with the following paragraph:

[0046] Referring once again to FIG. 2, in another embodiment, a verifier identifier (V) is also provided as input to the combination function 130. The verifier identifier (V) is a value associated with the identity of a particular verification computer (150) or group of verification computers. The use of the verifier identifier (V) allows the same user authentication device 120 (with the same secret (K)) to be used with verifiers operated by different entities without giving a particular entity information that could be used to impersonate the user to another entity. Techniques for implementing such systems are described in ~~co-pending~~ United States ~~Application Serial Patent No. 09/304,775~~ 6,985,583, the contents of which are incorporated herein by reference. In one embodiment, the verifier identifier (V) is a verifier-specific secret. In another embodiment, the verifier identifier (V) is public information that the user 110 can communicate to the device 120 so that the device 120 can be used with a particular verification computer 150.